



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

REC'D 16 APR 2004

WIPO PCT

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 23 FEV. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11354*03

REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 B V / 210502

REMISE DES PIÈCES DATE 11 DEC 2002 LIEU 54 INPI NANCY N° D'ENREGISTREMENT 0215623 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE 11 DEC. 2002 PAR L'INPI Vos références pour ce dossier (facultatif) 016711		NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE CABINET BALLOT 9, rue Claude Chappe Metz Technopôle 57070 METZ	
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N°	Date
ou demande de certificat d'utilité initiale		N°	Date
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/> N°	Date
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé de division entière ou de réduction modulaire sécurisé contre les attaques à canaux cachés.			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		GEMPLUS	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN			
Code APE-NAF			
Domicile ou siège	Rue	Avenue du Pic de Bertagne Parc d'Activités de GEMENOS	
	Code postal et ville	13420 GEMENOS	
	Pays	FRANCE	
Nationalité		française	
N° de téléphone (facultatif)		N° de télécopie (facultatif)	
Adresse électronique (facultatif)			
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

Remplir impérativement la 2^{ème} page



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 86

REÇU LE

12 DEC. 2002

BALLOT
METZ

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

REQUÊTE EN DÉLIVRANCE

page 1/2



N° 11354*03

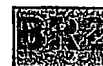
BR1

Cet imprimé est à remplir lisiblement à l'encre noire

09 540 0 W / 210502

REMISE DES PIÈCES DATE 11 DEC 2002 LIEU INPI NANCY N° D'ENREGISTREMENT 0215623 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI Vos références pour ce dossier (facultatif) 016711		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE CABINET BALLOT 9, rue Claude Chappe Metz Technopôle 57070 METZ	
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
ou demande de certificat d'utilité initiale		N° _____ Date _____	
Transformation d'une demande de brevet européen		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé de division entière ou de réduction modulaire sécurisé contre les attaques à canaux cachés.			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		GEMPLUS	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN		_____	
Code APE-NAF		_____	
Domicile ou siège	Rue	Avenue du Pic de Bertagne Parc d'Activités de GEMENOS	
	Code postal et ville	13420 GEMENOS	
	Pays	FRANCE	
Nationalité		française	
N° de téléphone (facultatif)		N° de télécopie (facultatif)	
Adresse électronique (facultatif)			
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

Remplir impérativement la 2^{ème} page



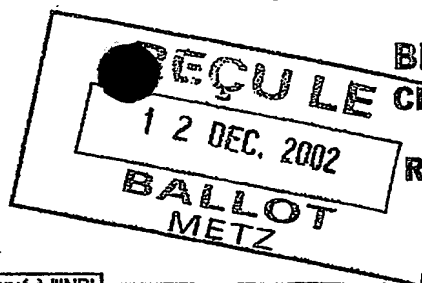
REMISE DES PIÈCES
DATE **11 DEC 2002**
LIEU **54 INPI NANCY**
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI

Réservé à l'INPI

0215623

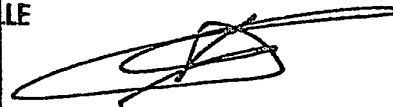
08 540 W / 210502

6 MANDATAIRE		
Nom	LECLAIRE	
Prénom	Jean-Louis	
Cabinet ou Société	CABINET BALLOT	
N° de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	9, rue Claude Chappe Metz Technopôle
	Code postal et ville	57 10 17 10 METZ
	Pays	FRANCE
N° de téléphone (facultatif)	03.87.74.81.36	
N° de télécopie (facultatif)	03.87.36.26.76	
Adresse électronique (facultatif)		
7 INVENTEUR(S)		Les inventeurs sont nécessairement des personnes physiques
Les demandeurs et les inventeurs sont les mêmes personnes	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)
Établissement immédiat ou établissement différé	<input checked="" type="checkbox"/> Établissement immédiat <input type="checkbox"/> Établissement différé	
Paiement échelonné de la redevance (en deux versements)	Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence): AG
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe	<input type="checkbox"/> Oui <input type="checkbox"/> Non	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Jean-Louis LECLAIRE - 93.4009		CABINET BALLOT CONSEILS EN PROPRIÉTÉ INDUSTRIELLE 9, rue Claude Chappe Technopôle Metz 2000 57070 METZ
		VISA DE LA PRÉFECTURE OU DE L'INPI



REMISE DES PIÈCES
DATE 11 DEC 2002
LIEU 54 INPI LANCY
N° D'ENREGISTREMENT 0215823
NATIONAL ATTRIBUÉ PAR L'INPI

DB 540.W / 210502

6 MANDATAIRE (s'il y a lieu)		
Nom	LECLAIRE	
Prénom	Jean-Louis	
Cabinet ou Société	CABINET BALLOT	
N° de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	9, rue Claude Chappe Metz Technopôle
	Code postal et ville	57 100 METZ
	Pays	FRANCE
N° de téléphone (facultatif)	03.87.74.81.36	
N° de télécopie (facultatif)	03.87.36.26.76	
Adresse électronique (facultatif)		
7 INVENTEUR (S)		Les inventeurs sont nécessairement des personnes physiques
Les demandeurs et les inventeurs sont les mêmes personnes		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>
Paiement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG <input type="text"/>
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		<input type="checkbox"/>
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		<input type="checkbox"/>
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Jean-Louis LECLAIRE - 93.4009		CABINET BALLOT CONSEILS EN PROPRIÉTÉ INDUSTRIELLE 9, rue Claude Chappe Technopôle Metz 2000 57070 METZ
		VISA DE LA PRÉFECTURE OU DE L'INPI 

PROCEDE DE DIVISION ENTIERE OU DE REDUCTION MODULAIRE
SECURISE CONTRE LES ATTAQUES A CANAUX CACHES

L'invention concerne un procédé de division entière ou de réduction modulaire sécurisé contre les attaques à canal caché, et notamment les attaques différentielles. L'invention peut être utilisée pour réaliser des opérations de division dans un procédé cryptographique plus général, par exemple un procédé cryptographique à clé secrète ou publique. Un tel procédé cryptographique peut par exemple être mis en œuvre dans des dispositifs électroniques tels que des cartes à puce.

10

La sécurité des procédés cryptographiques réside dans leur capacité à maintenir cachées les données confidentielles ou des données dérivées des données confidentielles qu'ils manipulent.

15

Un utilisateur malveillant peut éventuellement engager des attaques, visant à découvrir notamment des données confidentielles contenues et manipulées dans des traitements effectués par le dispositif de calcul exécutant un procédé cryptographique.

20

Parmi les attaques les plus connues, on peut citer les attaques à canaux cachés, simples ou différentielles. On entend par attaque à canal caché une attaque basée sur une grandeur physique mesurable de l'extérieur du dispositif, et dont l'analyse directe (attaque simple) ou l'analyse selon une méthode statistique (attaque différentielle) permet de découvrir des données manipulées dans des traitements réalisés dans le dispositif. Ces attaques ont notamment été dévoilées par Paul Kocher (Advances in Cryptology - CRYPTO'99, vol. 1666 of Lecture Notes in Computer Science, pp.388-397. Springer-Verlag, 1999).

30

Parmi les grandeurs physiques qui peuvent être exploitées à ces fins, on peut citer le temps d'exécution, la consommation en courant, le champ électromagnétique rayonné par la partie du composant utilisée pour exécuter le calcul, etc. Au cours de l'exécution d'un procédé, la manipulation d'un bit, c'est à dire son traitement par une instruction particulière, laisse une empreinte particulière sur la grandeur physique considérée, selon la valeur de ce bit et / ou selon l'instruction. Dit autrement, la trace (c'est-à-dire l'évolution dans le temps de la grandeur physique considérée) laissée par le composant exécutant le procédé est différente selon qu'on manipule un bit égal à 1 ou un bit égal à 0. Les attaques à canal caché sont basées sur cette faiblesse des procédés cryptographiques.

Les procédés cryptographiques utilisant comme opération de base une opération d'exponentiation modulaire de type $Y = X^D$, X , Y et D étant des nombres entiers ont été très largement étudiés ces dernières années. A titre d'exemple, on peut citer le procédé RSA, l'échange de clé selon Diffie-Hellman ou le procédé de signature DSA. Des progrès significatifs ont été réalisés pour protéger ces procédés contre les attaques à canaux cachés.

Par contre, certains procédés cryptographiques utilisent comme opération élémentaire une division entière de type $q = a \text{ div } b$ et / ou une réduction modulaire de type $r = a \text{ mod } b$, a et b étant deux opérands, q et r étant respectivement le quotient et le reste de la division entière de a par b . a et / ou b sont des données secrètes, par exemple des éléments d'une clé du procédé. Par exemple, le procédé de Barrett (P. Barret, "Implementing the RSA public key encryption algorithm on a standard digital signal processing", vol 263 of Lecture Notes in Computer Science, pp. 311-323,

Springer Verlag, 1987), le procédé de Quisquater (US patent 5,166,978, nov 92) ou le procédé RSA mis en œuvre selon le théorème des restes chinois (JJ Quisquater and C Couvreur, "Fast decipherment algorithm for RSA public key cryptosystem", Electronics Letters, vol 18, pp. 905-907, 5 Octobre 1982) sont des procédés cryptographiques utilisant une division entière comme opération élémentaire.

De tels procédés cryptographiques utilisant un 10 procédé de division entière et / ou un procédé de réduction modulaire sont sensibles aux attaques à canal caché, comme on va le voir dans l'exemple ci-dessous.

Un procédé connu pour mettre en œuvre à la fois une 15 division entière et une réduction modulaire est le procédé dit "papier crayon". Ce procédé reprend en pratique la méthode utilisée lorsqu'une telle opération est réalisée à la main. Ce procédé est rappelé ci-dessous.

20 Etant donné deux données $a = (a_{m-1}, \dots, a_0)$ de m bits et $b = (b_{n-1}, \dots, b_0)$ de n bits, n inférieur ou égal à m et $b_{n-1} \neq 0$, le procédé de division dit "papier crayon" calcule le quotient $q = a \text{ div } b$ et le reste $r = a \text{ div } b$. Pour cela, le procédé réalise successivement 25 plusieurs divisions d'un entier A de $n+1$ bits par l'entier b de n bits. On doit avoir en pratique $0 \leq A/b < 2$, ce qui est le cas chaque fois que $b_{n-1} \neq 0$.

Le reste r est un nombre de au plus n bits puisque $r < b$. Le quotient q est quant à lui un nombre de au plus 30 $m-n+1$ bits puisque $q = a \text{ div } b \leq a \text{ div } (b_{n-1} \cdot 2^{n-1}) = a \text{ div } 2^{n-1} = (a_{m-1}, \dots, a_{n-1})$ car $b \geq b_{n-1} \cdot 2^{n-1}$ et $(a_{m-1}, \dots, a_{n-1})$ est un nombre de $m-n+1$ bits. A la fin du procédé de division, le quotient q est mémorisé dans les $m-n+1$ bits de poids les plus faibles du registre contenant 35 initialement le nombre a . Le bit de poids le plus fort du reste r est mémorisé dans un registre de 1 bit utilisé

5 Comme on travaille en base 2, le bit de quotient de
la division entière $A \text{ div } b$ a seulement deux valeurs
possibles : 0 ou 1. Aussi une manière simple de réaliser
l'opération $A \text{ div } b$ consiste à soustraire b à A puis à
tester le résultat : si le résultat de $A - b$ est positif,
0 alors $A \text{ div } b = 1$, si le résultat de $A - b$ est
strictement négatif, alors $A \text{ div } b = 0$.

```

15      Entrée :   $a = (0, a_{m-1}, \dots, a_0)$ 
                $b = (b_{n-1}, \dots, b_0)$ 
      Sortie :   $q = a \text{ div } b$  et  $r = a \text{ mod } b$ 
       $A = (0, a_{m-1}, \dots, a_{m-n+1})$ 
      Pour  $j = 1$  à  $(m-n+1)$ , faire :
20           $a \leftarrow \text{SHL}_{m+1}(a, 1)$  ;  $\sigma \leftarrow \text{carry}$ 
           $A \leftarrow \text{SUB}_n(A, b)$  ;  $\sigma \leftarrow \sigma \text{ OU } \text{carry}$ 
          si  $(\neg \sigma = \text{VRAI})$  alors  $A \leftarrow \text{ADD}_n(A, b)$ 
                               sinon  $\text{lsb}(a) = 1$ 
      Fin Pour

```

25

30 Par abus de langage mais surtout par souci de clarté, et sauf précision explicite, on utilisera le même nom pour parler d'un registre et de son contenu. Ainsi on parlera du registre A pour parler du registre contenant la donnée A.

Le symbole "<-" et la notation y <- x sont utilisés
35 pour indiquer le chargement du contenu du registre x dans
un registre y dont le contenu est appelé également y.

A est un mot de n bits correspondant au contenu des n bits de poids les plus forts du registre contenant initialement la donnée a . Le registre A est bien sûr modifié à chaque itération, de même que le registre
 5 contenant initialement a .

σ indique si la soustraction a été effectuée à tort ou pas (ie si le bit de quotient doit être égal à 0 ou à 1).

$\neg\sigma$ est le complément à 1 (encore appelé négation)
 10 de la variable σ . VRAI est une constante, égale à 1 dans un exemple.

$\text{lsb}(a)$ est le bit de poids le plus faible du nombre a , également appelé bit le moins significatif de a .

$\text{SHL}_{m+1}(a, 1)$ est une opération de décalage à gauche
 15 de 1 bit dans le registre de $m+1$ bits contenant la donnée a , le bit sortant du registre étant mémorisé dans la variable carry et un bit égal à 0 étant entré en bit de poids le plus faible du registre contenant initialement la donnée a .

$\text{ADD}_n(A, b)$ est une opération d'addition des n bits
 20 du nombre b aux n bits du mot A . On notera que l'opération $\text{SHL}_n(a, 1)$ est équivalente à l'opération $\text{ADD}_n(a, a)$. Bien sûr l'addition $\text{ADD}_n(A, b)$ est réalisée en additionnant, dans un circuit d'addition approprié, le contenu de deux registres contenant respectivement A et
 25 b .

$\text{SUB}_n(A, b)$ est une opération de soustraction du nombre b au mot A . Bien sûr la soustraction $\text{SUB}_n(A, b)$ est réalisée en soustrayant, dans un circuit approprié, le
 30 contenu d'un registre contenant la donnée b au contenu du registre contenant le mot A .

En résumé, le procédé 1 réalise les étapes suivantes :

- si $a \leftarrow \text{SHL}_{m+1}(a, 1)$ génère une retenue ($\sigma = \text{carry}$
 35 $= 1$), cela signifie que $a_m = 1$ (avant décalage) et donc que b doit être soustrait à A .

- si $a_m = 0$ (avant décalage) et si $A \leftarrow \text{SUB}_n(A, b)$ génère une retenue (carry = 1), cela signifie que $A - b \geq 0$ avant la soustraction et donc b doit être soustrait à A .

5 - si $a \leftarrow \text{SHL}_{m+1}(a, 1)$ ne génère pas de retenue et
 si $A \leftarrow \text{SUB}_n(A, b)$ ne génère pas non plus de retenue
 (c'est-à-dire si, après mise à jour de σ , σ est FAUX (ou
 $\neg\sigma$ est VRAI, FAUX étant la négation de VRAI), alors cela
 signifie que $A - b < 0$ avant la soustraction et donc que
 10 b n'aurait pas dû être soustrait à A . Dans ce cas, le
 procédé réalise une opération d'addition $A \leftarrow \text{ADD}_n(A, b)$
 pour restaurer la valeur de A .

15 Le procédé 1 est sensible aux attaques à canal
 caché. En effet, on remarque sur le procédé 1 que, à
 chaque itération, selon la valeur de σ , c'est-à-dire
 selon la valeur du bit de quotient qui sera obtenu lors
 de l'itération en cours, on effectue soit une addition
 $\text{ADD}_n(A, b)$ soit une mise à 1 du bit de poids le plus
 20 faible du registre contenant la donnée a . La mise en
 œuvre et la durée d'exécution de ces deux opérations sont
 différentes et la trace qu'elles laissent lors de leur
 mise en œuvre est également différente. La trace globale
 laissée au cours d'une itération varie donc en fonction
 25 du bit de résultat obtenu lors de ladite itération. En
 mesurant et en étudiant par exemple la trace laissée par
 le composant lors de l'exécution du procédé complet, par
 exemple dans le cadre d'une attaque différentielle, il
 est alors possible de déterminer bit à bit la valeur des
 30 bits de résultat.

35 Le procédé 1 permet d'obtenir à la fois le résultat
 de la division entière ($q = a \text{ div } b$) et le reste de la
 division entière ($r = a \text{ mod } b$) qui est aussi le résultat
 d'une réduction modulaire. D'autres procédés connus
 présentant les mêmes inconvénients réalisent soit une
 division modulaire seule, soit une réduction modulaire

seule. De manière générale, un procédé de division est assez similaire à un procédé de réduction modulaire.

Un but de l'invention est de sécuriser un procédé
 5 de mise en œuvre d'une division et / ou d'une réduction modulaire.

Dans ce but, l'invention propose un procédé cryptographique au cours duquel on réalise une division entière de type $q = a \text{ div } b$ et / ou une réduction
 10 modulaire de type $r = a \text{ mod } b$, avec q un quotient, a un nombre de m bits, b un nombre de n bits, n inférieur ou égal à m et b_{n-1} non nul, b_{n-1} étant le bit de poids le plus fort du nombre b .

Selon l'invention, le procédé est caractérisé en ce
 15 qu'on masque le nombre a par un nombre aléatoire p avant de réaliser la division entière et / ou la réduction modulaire.

Le nombre a étant masqué par un nombre aléatoire, la trace (par exemple la consommation énergétique)
 20 laissée lors de l'exécution du procédé est différente à chaque exécution, de sorte qu'il n'est plus possible de mettre en œuvre une attaque à canal caché différentielle.

L'invention peut être appliquée par exemple au procédé 1 qui réalise à la fois une division et une
 25 réduction modulaire. L'invention peut être plus généralement appliquée à tout procédé qui réalise l'une ou l'autre des ces opérations.

Le nombre aléatoire p peut être modifié à chaque exécution du procédé, ou bien simplement après un nombre
 30 prédéfini d'exécutions du procédé. Le cas échéant, le dit nombre prédéfini est choisi de préférence relativement petit, par exemple un nombre de 32 à 64 bits.

Selon un mode de réalisation préféré de l'invention, pour masquer le nombre a , on ajoute, au
 35 nombre a , b fois le nombre aléatoire ($a \leftarrow a + b * p$). Pour cela, concrètement, le contenu du registre b est

multiplié par le nombre aléatoire p puis additionné au nombre a et le résultat de l'addition est ensuite mémorisé dans le registre contenant initialement le nombre a .

5 Puis, on réalise ensuite la division entière et /
ou la réduction modulaire souhaitée.

10 Dans le cas où une division entière est réalisée, le résultat de la division entière réalisée avec le nombre a masqué sous la forme $a + b \cdot p$ est égal à $a \text{ div } b + p$. Dans ce cas, après la division entière, on enlève au résultat de la division entière la contribution apportée par le nombre aléatoire p pour retrouver le résultat attendu de la division entière sur le nombre a , c'est-à-dire $a \text{ div } b$.

15 Dans le cas où réduction modulaire est réalisée, le résultat de l'opération $(a + b \cdot p) \bmod b$ est égal à $a \bmod b$, résultat attendu de la réduction modulaire sur le nombre a .

20 L'invention concerne également un composant électronique comprenant des moyens pour la mise en œuvre d'un procédé selon l'invention, tel que décrit ci-dessus. Les moyens de calcul programmés comprennent notamment plusieurs registres pour mémoriser les nombres a et b .

25 Enfin, l'invention concerne une carte à puce comprenant un composant ayant les caractéristiques décrites ci-dessus.

REVENDEICATIONS

1. Procédé cryptographique au cours duquel on réalise une division entière de type $q = a \text{ div } b$ et / ou une réduction modulaire de type $r = a \text{ mod } b$, avec q un quotient, a un nombre de m bits, b un nombre de n bits, n inférieur ou égal à m et b_{n-1} non nul, b_{n-1} étant le bit de poids le plus fort du nombre b , caractérisé en ce qu'on masque le nombre a par un nombre aléatoire p avant de réaliser la division entière et / ou la réduction modulaire.

10

2. Procédé selon la revendication 1, au cours duquel, pour masquer le nombre a , on ajoute au nombre a , b fois le nombre aléatoire p ($a \leftarrow a + b * p$).

15

3. Procédé selon la revendication 1 ou la revendication 2, dans lequel, après avoir réalisé une division entière, on enlève au résultat de la division entière la contribution apportée par le nombre aléatoire p .

20

4. Procédé selon la revendication 3 en combinaison avec la revendication 2, au cours duquel, pour enlever la contribution apportée par le nombre aléatoire p , on soustrait le dit nombre aléatoire p au résultat de la division entière.

25

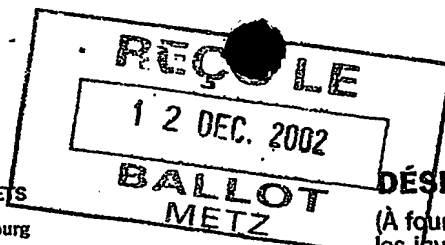
5. Procédé selon l'une des revendications 1 à 4, au cours duquel le nombre aléatoire p est modifié à chaque mise en œuvre du procédé.

30

6. Procédé selon l'une des revendications 1 à 4, au cours duquel le nombre aléatoire p est modifié après un nombre prédéterminé de mise en œuvre du procédé.

7. Composant électronique comprenant des moyens
pour la mise en œuvre d'un procédé selon l'une des
revendication précédente, les moyens de calcul programmés
5 comprenant notamment plusieurs registres pour mémoriser
~~les nombres a et b.~~

8. Carte à puce comprenant un composant selon la
revendication précédente.



BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

DÉSIGNATION D'INVENTEUR(S) Page N° ... / ...

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

INV

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier (facultatif)

N° D'ENREGISTREMENT NATIONAL

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de division entière ou de réduction modulaire sécurisé contre les attaques à canaux cachés.

LE(S) DEMANDEUR(S) :

GEMPLUS
Avenue du Pic de Bertagne
Parc d'activités de Gemenos
13420 GEMENOS
FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1	Nom	JOYE
	Prénoms	Marc
Adresse	Rue	19, rue Voltaire
	Code postal et ville	83640 SAINT-ZACHARIE
Société d'appartenance (facultatif)		
2	Nom	
	Prénoms	
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
3	Nom	
	Prénoms	
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		

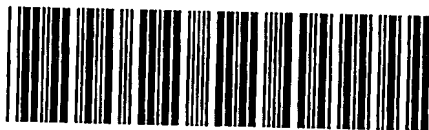
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Jean-Louis LECLAIRE - 93.4009

CABINET BALLOT
CONSEILS EN PROPRIÉTÉ INDUSTRIELLE
9, rue Claude Chappe
Technopôle Metz 2000
57070 METZ

PCT Application
PCT/FR2003/003681



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.